WHAT IS CLAIMED IS:

1. A security management apparatus comprising:

a security diagnostic unit for making a security diagnosis on a basis of security information obtained from a security information providing unit for providing information concerning security in a network and further on a basis of machine information obtained from at least one network machine connected to a network to judge a type of security-related processing to be executed for said network machine or a predetermined network including said network machine and also judge whether or not the security-related processing needs to be executed; and

a security execution unit for executing predetermined security measure processing for said network machine or the predetermined network including said network machine on a basis of a result of diagnosis made by said security diagnostic unit.

2. A security management apparatus according to claim 1, wherein said security diagnostic unit further uses machine-related information obtained from a machine-related information storage unit containing predetermined information about network machines that are connected to said network or may be connected to said network to judge a type of security-related processing to be executed for said network machine or the predetermined network including said network machine and also judge whether or not the security-related processing needs to be executed.

3. A security management apparatus according to claim 2, wherein the machine-related information stored in said machine-related information storage unit is information specifying a security policy.

4. A security management apparatus according to claim 1, further comprising:

a connection request accepting unit for accepting a connection request from a newly introduced network machine;

wherein when said connection request accepting unit accepts a connection request from a newly introduced network machine, said security diagnostic unit assigns an address to said newly introduced network machine after placing it in an isolated state and judges whether or not to execute processing for unisolating said newly introduced network machine as said security-related processing on a basis of said machine information and said security information.

5. A security management apparatus according to claim 1, further comprising:

a connection request accepting unit for accepting a connection request from a newly introduced network machine;

wherein when said connection request accepting unit accepts a connection request from a newly introduced network machine, said security diagnostic unit receives machine information from said newly introduced network machine and judges whether or not to execute processing for assigning an address to said newly introduced network machine as said security-related processing on a basis of said machine information and said security information.

6. A security management apparatus comprising:

a security diagnostic unit for making a security diagnosis on a basis of machine information obtained from at least one network machine connected to

a network and further on a basis of machine-related information obtained from a machine-related information storage unit containing predetermined information about network machines that are connected to said network or may be connected to said network to judge a type of security-related processing to be executed for said network machine or a predetermined network including said network machine and also judge whether or not the security-related processing needs to be executed; and

a security execution unit for executing predetermined security measure processing for said network machine or the predetermined network including said network machine on a basis of a result of diagnosis made by said security diagnostic unit.

7. A security management apparatus according to claim 6, wherein said machine-related information includes information indicating behavior of computer viruses, and said machine information includes at least either one of a hash value of a predetermined file and a virus scan result; and

said security diagnostic unit judges whether or not a predetermined network machine needs to be isolated, and said security execution unit executes processing for isolating said network machine when said security diagnostic unit judges that said network machine needs to be isolated.

8. A security management apparatus according to claim 6, further comprising:

a network monitor for monitoring communications on said network machines;

wherein said machine-related information is information concerning a network machine profile;

said security diagnostic unit judges whether or not a predetermined

network machine needs to be isolated on a basis of monitor information obtained from said network monitor and said machine information and further said network machine profile information; and

said security execution unit executes processing for isolating said network machine when said security diagnostic unit judges that said network machine needs to be isolated.

9. A security management apparatus according to claim 6, wherein said security diagnostic unit identifies a range of damage and determines a range of isolation.

10. A security management apparatus according to claim 6, further comprising:

a recovery unit for repairing a network machine or network having received predetermined damage on a basis of a result of diagnosis made by said security diagnostic unit.

11. A security management apparatus according to claim 6, further comprising:

an unisolating unit for canceling isolation when damage repair has been made.

12. A security management apparatus according to claim 6, wherein said machine information includes a notice of a change in equipment configuration and at least information concerning the equipment configuration that may be changed, and said machine-related information includes equipment configuration information specifying whether or not the network machine is usable in said network.

13. A security management system comprising:

a security information providing apparatus for providing security information concerning security in a network;

a machine-related information database containing predetermined information about network machines that are connected to said network or may be connected to said network;

a preventive system for judging whether or not there is damage to at least one network machine connected to a network or damage to a predetermined network including said network machine or whether or not preventive measures need to be executed for said network machine or said predetermined network on a basis of security information obtained from said security information providing apparatus and machine-related information obtained from said machine-related information database and further machine information obtained from said network machine; and

a recovery system for executing recovery processing when there is predetermined damage, or taking preventive measures on a basis of judgment made by said preventive system.

14. A security management system according to claim 13, wherein a plurality of said preventive systems or a plurality of said recovery systems are provided, and a management center for generally managing these systems is provided.

15. A security management system according to claim 13, wherein said preventive system and said recovery system are provided on a side of an owner of said security information providing apparatus.

16. A security management system according to claim 13, wherein

said preventive system is provided on a side of an owner of said security information providing apparatus, and said recovery system is provided on a side of a management service provider who provides management services.

17. A security management system according to claim 13, wherein said preventive system and said recovery system are provided on a side of a management service provider who provides management services.

18. A security management system according to claim 13, wherein predetermined information obtained by said recovery system is fed back to said preventive system as new security information.

19. A security management method comprising the steps of:

obtaining security information concerning security in a network;

obtaining machine information from at least one network machine connected to a network;

making a security diagnosis on a basis of said security information and said machine information to judge a type of security-related processing to be executed for said network machine or a predetermined network including said network machine and also judge whether or not the security-related processing needs to be executed; and

executing predetermined security measure processing for said network machine or the predetermined network including said network machine on a basis of a result of diagnosis made by said security diagnostic step.

20. A security management method according to claim 19, further comprising the step of obtaining machine-related information from a machine-related information storage unit containing predetermined information about

network machines that are connected to said network or may be connected to said network;

wherein said security diagnostic step makes said security diagnosis on a basis of said machine-related information as well as said security information and said machine information.

21. A security management method comprising the steps of:

obtaining machine information from at least one network machine connected to a network;

obtaining machine-related information from a machine-related information storage unit containing predetermined information about network machines that are connected to said network or may be connected to said network;

making a security diagnosis on a basis of said machine information and said machine-related information to judge a type of security-related processing to be executed for said network machine or a predetermined network including said network machine and also judge whether or not the security-related processing needs to be executed; and

executing predetermined security measure processing for said network machine or the predetermined network including said network machine on a basis of a result of diagnosis made by said security diagnostic step.

22. A security management program for instructing a computer to execute security management, said program comprising the steps of:

obtaining security information concerning security in a network;

obtaining machine information from at least one network machine connected to a network;

making a security diagnosis on a basis of said security information and

said machine information to judge a type of security-related processing to be executed for said network machine or a predetermined network including said network machine and also judge whether or not the security-related processing needs to be executed; and

executing predetermined security measure processing for said network machine or the predetermined network including said network machine on a basis of a result of diagnosis made by said security diagnostic step.

23. A security management program according to claim 22, further comprising the step of obtaining machine-related information from a machine-related information storage unit containing predetermined information about network machines that are connected to said network or may be connected to said network;

wherein said security diagnostic step makes said security diagnosis on a basis of said security information and said machine information and further said machine-related information.

24. A security management program for instructing a computer to execute security management, said program comprising the steps of:

obtaining machine information from at least one network machine connected to a network;

obtaining machine-related information from a machine-related information storage unit containing predetermined information about network machines that are connected to said network or may be connected to said network;

making a security diagnosis on a basis of said machine information and said machine-related information to judge a type of security-related processing to be executed for said network machine or a predetermined

network including said network machine and also judge whether or not the security-related processing needs to be executed; and

executing predetermined security measure processing for said network machine or the predetermined network including said network machine on a basis of a result of diagnosis made by said security diagnostic step.